

Network security system for wireless communication networks, has controller that extracts non-registered access points by comparing list of previously registered access points with lists dispatched by clients

Patent Assignee: IBM CORP; INT BUSINESS MACHINES CORP

Inventors: FUJII K; ITO M; ITOH M; MATSUNAGA K

Patent Family (3 patents, 2 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
US 20030117985	A1	20030626	US 2002248116	A	20021219	200362	B
JP 2003198571	A	20030711	JP 2001395303	A	20011226	200362	E
JP 3792154	B2	20060705	JP 2001395303	A	20011226	200644	E

Priority Application Number (Number Kind Date): JP 2001395303 A 20011226

Patent Details

Patent Number	Kind	Language	Pages	Drawings	Filing Notes
US 20030117985	A1	EN	14	7	
JP 2003198571	A	JA	11		
JP 3792154	B2	JA	14		Previously issued patent JP 2003198571

Alerting Abstract: US A1

NOVELTY - The system has clients (10a-e) that search for neighbor access points in order to establish wireless connection to a local area network (LAN) and dispatch a list of access points obtained to a controller (20), as a result of the search. The controller extracts non- registered access points by comparing a list of previously registered access points with the lists dispatched by the clients.

DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

1.an access point recognizing method 2.a method of checking an access point.

USE - Used for wireless communication networks.

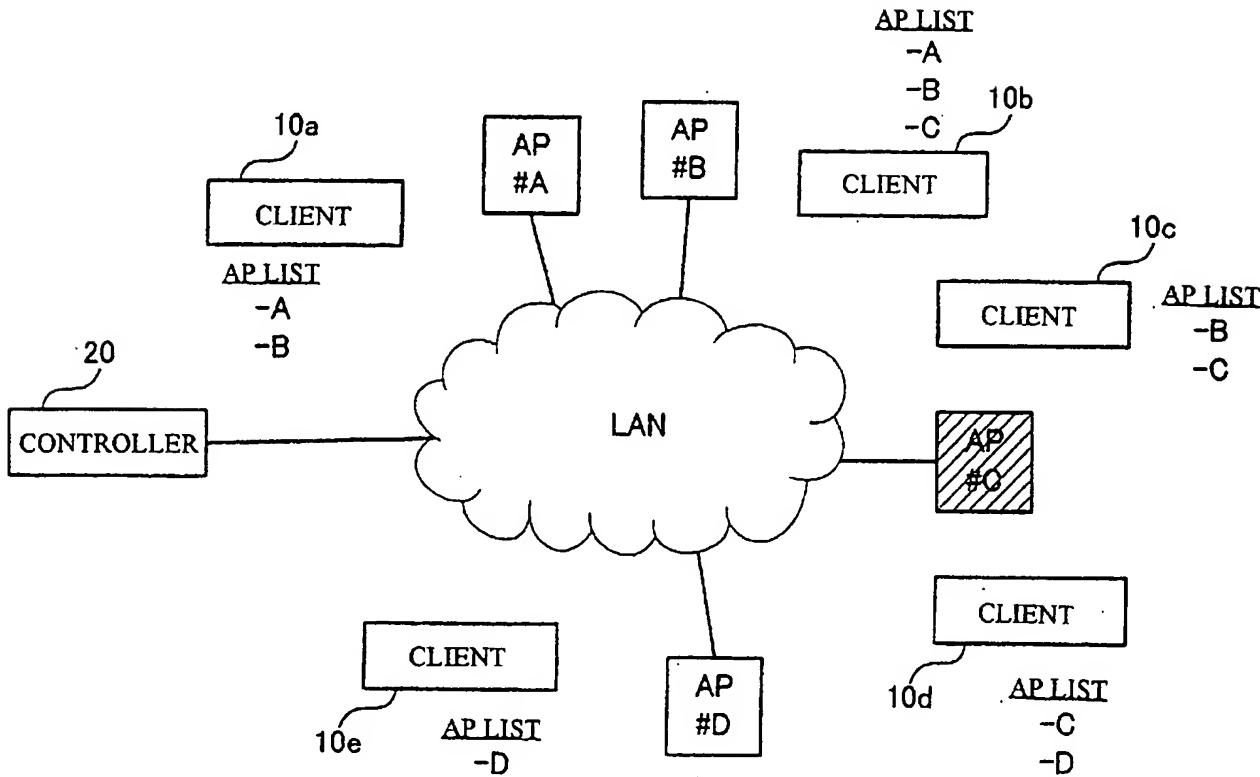
ADVANTAGE - The apparatus can detect illegal access points within the network according to the information on the retrieved access points, thereby enhancing security in the network.

DESCRIPTION OF DRAWINGS - The drawing shows a configuration of a local area network system.

10a-e Clients

20 Computer.

Main Drawing Sheet(s) or Clipped Structure(s)



International Classification (Main): H04L-012/28 **(Additional/Secondary):** G06F-013/00, H04Q-007/38

International Patent Classification

IPC	Level	Value	Position	Status	Version
H04L-0012/28	A	I		R	20060101
H04L-0012/28	A	I	F	B	20060101
H04L-0029/06	A	I		R	20060101
H04Q-0007/38	A	I	L	B	20060101
H04L-0012/28	C	I		R	20060101
H04L-0029/06	C	I		R	20060101

US Classification, Issued: 370328000, 370338000

Original Publication Data by Authority

Japan

Publication Number: JP 2003198571 A (Update 200362 E)

Publication Date: 20030711

NETWORK SECURITY SYSTEM, COMPUTER SYSTEM, RECOGNIZING PROCESSING METHOD FOR ACCESS POINT, CHECK METHOD FOR ACCESS POINT, PROGRAM, STORAGE MEDIUM AND DEVICE FOR WIRELESS LAN

Assignee: INTERNATL BUSINESS MACH CORP (IBMC)

Inventor: FUJII KAZUO MATSUNAGA KOZO ITO MASAHIRO

Language: JA (11 pages)

Application: JP 2001395303 A 20011226 (Local application)

Original IPC: H04L-12/28(A) G06F-13/00(B) H04Q-7/38(B)

Current IPC: H04L-12/28(A) G06F-13/00(B) H04Q-7/38(B)|JP 3792154 B2 (Update 200644 E)

Publication Date: 20060705

Assignee: IBM CORP (IBMC)

Language: JA (14 pages)

Application: JP 2001395303 A 20011226 (Local application)

Related Publication: JP 2003198571 A (Previously issued patent)

Original IPC: H04L-12/28(B,I,H,JP,20060101,20060615,A,F) H04Q-7/38
(B,I,H,JP,20060101,20060615,A,L)

Current IPC: H04L-12/28(B,I,H,JP,20060101,20060615,A,F) H04Q-7/38
(B,I,H,JP,20060101,20060615,A,L)

United States

Publication Number: US 20030117985 A1 (Update 200362 B)

Publication Date: 20030626

NETWORK SECURITY SYSTEM, COMPUTER, ACCESS POINT RECOGNIZING METHOD, ACCESS POINT CHECKING METHOD, PROGRAM, STORAGE MEDIUM, AND WIRELESS LAN DEVICE

Assignee: INTERNATIONAL BUSINESS MACHINES CORPORATION, New Orchard Road, Armonk, 10504 New York, US (IBMC)

Inventor: FUJII, KAZUO, 1951-41, Tohkaichiba-Midori-ku, Yokohama-shi, Kanagawa-ken, JP

Nationality: JP ITOH, MASAHIRO, 5-3-1-401, Fukuda, Yamato-shi, Kanagawa-ken, JP Nationality:

JP MATSUNAGA, KOZO, 7-8-1-202, Kamitsuruma, Sagamihara, Sagamihara-shi, Kanagawa-ken, JP

Nationality: JP

Language: EN (14 pages, 7 drawings)

Application: US 2002248116 A 20021219 (Local application)

Priority: JP 2001395303 A 20011226

Original IPC: H04Q-7/24(A)

Current IPC: H04L-12/28(R,I,M,EP,20060101,20051008,A) H04L-12/28

(R,I,M,EP,20060101,20051008,C) H04L-29/06(R,I,M,EP,20060101,20051008,A) H04L-29/06
(R,I,M,EP,20060101,20051008,C)

Original US Class (secondary): 370328 370338

Original Abstract: Abstract of the DisclosureIn a network security system, clients search for neighbor access points (APs) in order to establish wireless connections to a LAN. As a result of the search, each of the clients dispatches a list of access points obtained to a controller. The controller detects non-registered access points by comparing a list of previously registered access points with the lists dispatched by the clients.

Claim: What is Claimed is: 1.Apparatus comprising: * ***1.*^{*} a client permitted to establish a wireless connection to a ne twork through an access point; and * a controller permitted to receive data dispatched by said client, thr ough said network, * wherein said client scans electromagnetic waves within bands permitte d to be used for wireless communication, and dispatches to said contr oller identification information on access points detected as a resul t of the scan, and * said controller stores said identification information on access poin ts permitted to access said network, and on the basis of the

identification information on the permitted access points and said identification information dispatched by said client, extracts non-registered access points that are not registered as permitted access points.

Derwent World Patents Index

© 2006 Derwent Information Ltd. All rights reserved.

Dialog® File Number 351 Accession Number 13566299

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-198571

(P2003-198571A)

(43)公開日 平成15年7月11日 (2003.7.11)

(51) Int.Cl.⁷
H 04 L 12/28
G 06 F 13/00
H 04 Q 7/38

識別記号
3 1 0
5 1 0

F I
H 04 L 12/28
G 06 F 13/00
H 04 B 7/26

テマコード(参考)
3 1 0 5 K 0 3 3
5 1 0 A 5 K 0 6 7
1 0 9 R

審査請求 有 請求項の数18 OL (全 11 頁)

(21)出願番号 特願2001-395303(P2001-395303)
(22)出願日 平成13年12月26日 (2001.12.26)

(71)出願人 390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
INTERNATIONAL BUSINESS MACHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州
アーモンク ニュー オーチャード ロード
(74)代理人 100086243
弁理士 坂口 博 (外3名)

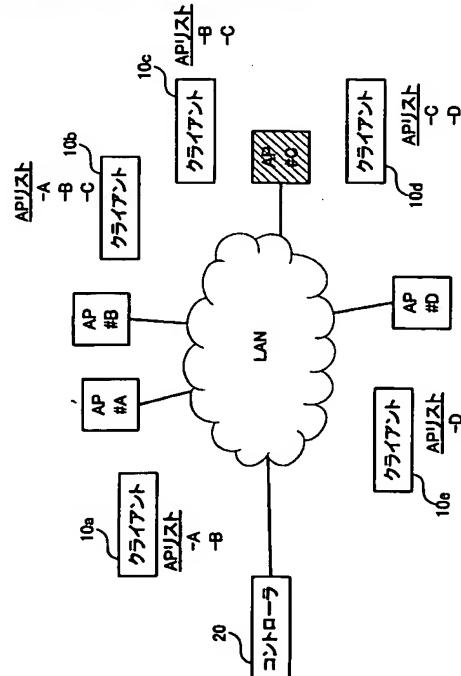
最終頁に続く

(54)【発明の名称】 ネットワークセキュリティシステム、コンピュータ装置、アクセスポイントの認識処理方法、アクセスポイントのチェック方法、プログラム、記憶媒体および無線LAN用デバイス

(57)【要約】

【課題】 無線LANにおいてセキュリティを強化することができるシステムを提供する。

【解決手段】 ネットワークセキュリティシステムでは、クライアント10a～eは無線を通じてLANに接続するため、近くのアクセスポイント(AP)をサーチする。サーチの結果、得られたアクセスポイントのリストをコントローラ20へ送出する。コントローラ20では、予め登録されたアクセスポイントのリストと、各クライアント10a～eから送出されたリストとを比較し、未登録のアクセスポイントを検出する。



【特許請求の範囲】

【請求項1】 アクセスポイントを介してネットワークへの無線接続を許可されたクライアントと、前記ネットワークを介して前記クライアントから送出されたデータの受信が可能なコントローラと、を備え、前記クライアントは、無線通信可能な帯域の電波をスキャンし、その結果検出されたアクセスポイントの識別情報を前記コントローラへ送出し、前記コントローラは、前記ネットワークに対してアクセスが許可された許可アクセスポイントの識別情報を格納し、当該許可アクセスポイントの当該識別情報と前記クライアントから送出された前記識別情報とに基づき、検出された前記アクセスポイントのうち、当該許可アクセスポイントとして登録されていない未登録アクセスポイントを抽出することを特徴とするネットワークセキュリティシステム。

【請求項2】 前記クライアントは、前記無線接続には使用しない前記アクセスポイントの前記識別情報を前記コントローラに送出することを特徴とした請求項1記載のネットワークセキュリティシステム。

【請求項3】 前記クライアントは、前記アクセスポイントから受信した信号の強度を前記コントローラへ送出し、前記コントローラは、前記強度に基づき、前記未登録アクセスポイントの設置エリアを推定することを特徴とする請求項1記載のネットワークセキュリティシステム。

【請求項4】 ネットワークに接続されたアクセスポイントと無線通信が可能なコンピュータ装置であって、アクセスポイントから発生する電波に基づいて、当該アクセスポイントの識別情報を認識する認識部と、前記認識部で認識された前記識別情報を記憶する記憶部と、

前記記憶部に記憶された前記識別情報を前記ネットワークを介して送出する送出部と、を備えたことを特徴とするコンピュータ装置。

【請求項5】 前記送出部は、所定時間毎に、または前記ネットワークを介した要求に応じて、前記識別情報を送出することを特徴とする請求項4記載のコンピュータ装置。

【請求項6】 アクセスポイントを介してネットワークへの無線接続を許可されたクライアントと、当該ネットワークを介してデータの送受信が可能なコントローラであって、

前記ネットワークに対してアクセスが許可された許可アクセスポイントの許可リストを格納する格納部と、前記クライアントにより無線通信可能な帯域の電波がスキャンされることにより認識された認識アクセスポイントの認識リストを収集する収集部と、前記許可リストおよび前記認識リストに基づき、前記認識リストに含まれる前記認識アクセスポイントのうち、

前記許可リストに含まれていない未登録アクセスポイントを抽出する抽出部と、を備えたことを特徴とするコンピュータ装置。

【請求項7】 前記ネットワークにおける前記許可アクセスポイントの設置位置情報を格納する設置位置情報格納部と、

前記認識アクセスポイントから発生した信号の強度を収集する信号収集部と、

前記強度と前記設置位置情報に基づき、前記未登録アクセスポイントの設置位置を算出する算出部と、

をさらに備えたことを特徴とする請求項6記載のコンピュータ装置。

【請求項8】 ネットワークに接続されたアクセスポイントと無線通信可能なコンピュータ装置におけるアクセスポイントの認識処理方法であって、無線通信可能な帯域の電波をスキャンするステップと、前記スキャンによって検出されたアクセスポイントのリストを取得するステップと、取得した前記リストを前記ネットワークを介して送出するステップと、を有することを特徴とするアクセスポイントの認識処理方法。

【請求項9】 前記アクセスポイントから発生する信号の強度を取得するステップと、前記強度を前記ネットワークを介して送出するステップと、をさらに有することを特徴とする請求項8記載のアクセスポイントの認識処理方法。

【請求項10】 コンピュータ装置を無線によりネットワークへ繋ぐため、当該ネットワークに接続されるアクセスポイントをチェックする方法であって、前記ネットワークに対してアクセスが許可されたアクセスポイントの許可リストを取得するステップと、前記コンピュータ装置により認識されたアクセスポイントの検出リストを取得するステップと、前記許可リストと前記検出リストを比較し、当該検出リストに含まれる前記アクセスポイントのうち、当該許可リストに含まれない未登録アクセスポイントを認識するステップと、

を有することを特徴とするアクセスポイントのチェック方法。

【請求項11】 前記許可リストに含まれる前記アクセスポイントの設置箇所を登録するステップと、前記コンピュータ装置のスキャンによって検出された前記アクセスポイントからの信号の強度を取得するステップと、

前記強度に基づき、前記未登録アクセスポイントの設置箇所を算出するステップと、をさらに有することを特徴とする請求項10記載のアクセスポイントのチェック方法。

【請求項12】 ネットワークに接続されたアクセスポイントと無線通信可能なコンピュータ装置に実行させるためのプログラムであって、

無線通信可能な帯域の電波をスキャンする手順と、前記スキャンによって検出されたアクセスポイントのリストを記録する手順と、前記リストを前記ネットワークを介して送出する手順と、を備えたことを特徴とするコンピュータ装置に実行させるためのプログラム。

【請求項13】 前記アクセスポイントから発生する振動の強度を取得する手順と、前記強度を前記ネットワークを介して送出する手順と、をさらに備えたことを特徴とする請求項12記載のコンピュータ装置に実行させるためのプログラム。

【請求項14】 コンピュータ装置を無線によりネットワークへ繋ぐため、当該ネットワークに接続されるアクセスポイントをチェックするプログラムであって、前記ネットワークに対してアクセスが許可されたアクセスポイントの許可リストを取得する手順と、前記コンピュータ装置により認識されたアクセスポイントの検出リストを取得する手順と、前記許可リストと前記検出リストを比較し、当該検出リストに含まれる前記アクセスポイントのうち、当該許可リストに含まれない未登録アクセスポイントを認識する手順と、を有することを特徴とするコンピュータ装置に実行させるためのプログラム。

【請求項15】 前記許可リストに含まれる前記アクセスポイントの設置箇所を登録する手順と、

前記コンピュータ装置のスキャンによって検出された前記アクセスポイントからの信号の強度を取得する手順と、

前記強度に基づき、前記未登録アクセスポイントの設置箇所を算出する手順と、をさらに有することを特徴とする請求項14記載のコンピュータ装置に実行させるためのプログラム。

【請求項16】 ネットワークに接続されたアクセスポイントと無線通信可能なコンピュータ装置に実行せるためのプログラムを、当該コンピュータ装置が読み取り可能に記憶した記憶媒体であって、無線通信可能な帯域の電波をスキャンする機能と、

前記スキャンによって検出されたアクセスポイントのリストを記録する機能と、前記リストを前記ネットワークを介して送出する機能と、

を前記コンピュータ装置に実現させるプログラムを記憶したことを特徴とする記憶媒体。

【請求項17】 コンピュータ装置を無線によりネットワークへ繋ぐため、当該ネットワークに接続されるア

セスポイントをチェックさせるためのプログラムを、当該コンピュータ装置が読み取り可能に記憶した記憶媒体であって、

前記ネットワークに対してアクセスが許可されたアクセスポイントの許可リストを取得する機能と、前記コンピュータ装置により認識されたアクセスポイントの検出リストを取得する機能と、

前記許可リストと前記検出リストを比較し、当該検出リストに含まれる前記アクセスポイントのうち、当該許可リストに含まれない未登録アクセスポイントを認識する機能と、

を前記コンピュータ装置に実現させるプログラムを記憶したことを特徴とする記憶媒体。

【請求項18】 無線LANを介してネットワークとデータの送受信を行うため、コンピュータ装置に接続可能な無線LAN用デバイスであって、

アクセスポイントをサーチするためのスキャンを行うスキャン部と、

前記スキャン部によって検出された前記アクセスポイントのIDを記録するID記録部と、

前記記録部に記録された前記IDを前記ネットワークへ送出する送出部と、

を備えたことを特徴とする無線LAN用デバイス。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ネットワークセキュリティシステム等に関し、より詳しくは不正に接続されたアクセスポイントを検出できるネットワークセキュリティシステム等に関する。

【0002】

【従来の技術】 従来、職場や家庭内等、様々な箇所でコンピュータ装置が広く使用されている。汎用されているコンピュータ装置の種類としては、机等の所定の場所にほぼ固定されて使用されるデスクトップ型PC(Personal Computer)や、可搬性を考慮して比較的小型に設計されたノートブック型PC、PDA(Personal Digital Assistant)等を挙げることができる。これらコンピュータ装置においては、ネットワークを介して外部とのデータの送受信が行われているが、特に近年では無線LANモジュールを用いてデータの送受信が無線により行われている。この無線LANモジュールが導入されると、コンピュータ装置はネットワークに接続された無線基地局(以下、アクセスポイントという)とデータの送受信ができる限り、移動先においても外部とのデータの送受信を簡単に行うことができる。

【0003】 ところで、このようなアクセスポイントとのデータの送受信においては、接続を許可されていないコンピュータ装置がネットワークに不正に接続し、データを盗むことがしばしば起きている。そこで、ネットワークにおいてこのような不正な接続を防ぐために様々な

処理が行われており、例えば、WEP (Wired Equivalent Privacy) と呼ばれる手法では、64または128bitのキーに基づいて、データを暗号化し、エラーや改ざんの有無をチェックすることで不正な接続を防止する。しかし、WEPでは、キーを不正に入手されてしまった場合、暗号化されたデータは容易に復号化されてしまう。一方、MAC (Media Access Control) Address Filteringと呼ばれる手法では、予めアクセスを許可されたコンピュータ装置のMACアドレス以外のMACアドレスを有するコンピュータ装置のアクセスを禁止している。しかし、MACアドレスを偽造することは比較的簡単にできてしまうので、許可されていないコンピュータ装置の不正なアクセスを完全に防止する機能を期待するのは難しい。

【0004】そこで、最近では複数の手法を組み入れた方法が採用されている。例えば、ユーザIDとパスワードにより所定のユーザの接続を管理し、MAC (Media Access Control) Address Filteringにより所定のコンピュータ装置の接続を管理し、さらに802.1xと呼ばれる手法によりデータの暗号化を行う。802.1xとは、コンピュータ装置とアクセスポイントとのセッション毎に、上記のWEPキーを動的に生成し、そのWEPキーを利用して認証を行う。すなわちこの方法では、セッション毎にキーが変わるので、万が一キーが盗まれても、次のセッションにおいてはそのキーは無効となる。

【0005】

【発明が解決しようとする課題】しかしながら、不正なアクセスポイントがネットワークに接続されることで、以上述べた方法も無効になってしまう場合がある。一般にWEPキーは、コンピュータ装置またはアクセスポイントのメモリ内に保存され、WEPキーの認証はアクセスポイント側から一方向に行われる。そのため、アクセスポイント側はコンピュータ装置を使用するユーザを認証するが、ユーザ側がアクセスポイントを認証することは殆ど不可能である。したがって、不正にアクセスポイントが設置された場合、そこからデータを不正に入手されたり、正当なユーザのクライアントが乗っ取られたりしてしまう可能性がある。

【0006】また、WEPキーの認証を両方向、すなわちコンピュータ装置側とアクセスポイント側が相互に行うことも不可能ではないが、サーバやクライアントとは別の認証サーバをネットワーク上に設置しなければならず、また認証の設定や不正アクセスの管理に大変手間がかかる。

【0007】本発明は、上記のような技術的課題に基づいてなされたもので、無線通信を行うネットワークにおいてセキュリティを高めることができたネットワークセキュリティシステム等を提供することを主たる目的とする。

【0008】

【課題を解決するための手段】かかる目的のもと、本発明のネットワークセキュリティシステムは、アクセスポイントを介してネットワークへの無線接続を許可されたクライアントと、ネットワークを介してクライアントから送出されたデータの受信が可能なコントローラとを備え、クライアントは、無線通信可能な帯域の電波をスキャンし、その結果検出されたアクセスポイントの識別情報をコントローラへ送出し、コントローラは、ネットワークに対してアクセスが許可された許可アクセスポイントの識別情報を格納し、許可アクセスポイントの識別情報とクライアントから送出された識別情報とに基づき、検出されたアクセスポイントのうち、許可アクセスポイントとして登録されていない未登録アクセスポイントを抽出することを特徴とするものである。このネットワークセキュリティシステムでは、予め許可されたアクセスポイントと、クライアントが検出したアクセスポイントとを比較することにより、登録されていないアクセスポイントを見つけ出すことが可能である。

【0009】このネットワークセキュリティシステムでは、クライアントは、無線接続には使用しないアクセスポイントの識別情報をコントローラに送出することが可能である。また、クライアントは、アクセスポイントから受信した信号の強度をコントローラへ送出し、コントローラは、強度に基づき、未登録アクセスポイントの設置エリアを推定することができる。

【0010】また、本発明はコンピュータ装置として捉えることもできる。このコンピュータ装置は、ネットワークに接続されたアクセスポイントと無線通信が可能なコンピュータ装置であって、アクセスポイントから発生する電波に基づいて、アクセスポイントの識別情報を認識する認識部と、認識部で認識された識別情報を記憶する記憶部と、記憶部に記憶された識別情報を、ネットワークを介して送出する送出部と、を備えたことを特徴とするものである。ここで、送出部は、所定時間毎に、またはネットワークを介した要求に応じて、識別情報を送出することができる。

【0011】さらに本発明のコンピュータ装置は、アクセスポイントを介してネットワークへの無線接続を許可されたクライアントと、ネットワークを介してデータの送受信が可能なコントローラであって、ネットワークに対してアクセスが許可された許可アクセスポイントの許可リストを格納する格納部と、クライアントにより無線通信可能な帯域の電波がスキャンされることにより認識された認識アクセスポイントの認識リストを収集する収集部と、許可リストおよび認識リストに基づき、認識リストに含まれる認識アクセスポイントのうち、許可リストに含まれていない未登録アクセスポイントを抽出する抽出部と、を備えたことを特徴とするものである。

【0012】このコンピュータ装置は、ネットワークに

おける許可アクセスポイントの設置位置情報を格納する設置位置情報格納部と、認識アクセスポイントから発生した信号の強度を収集する信号収集部と、強度と設置位置情報に基づき、未登録アクセスポイントの設置位置を算出する算出部と、をさらに備えることができる。

【0013】その他、本発明はアクセスポイントの認識処理方法として捉えることができる。このアクセスポイントの認識処理方法は、ネットワークに接続されたアクセスポイントと無線通信可能なコンピュータ装置におけるアクセスポイントの認識処理方法であって、無線通信可能な帯域の電波をスキャンするステップと、スキャンによって検出されたアクセスポイントのリストを取得するステップと、取得したリストをネットワークを介して送出するステップと、アクセスポイントから発生する信号の強度を取得するステップと、強度をネットワークを介して送出するステップと、を有することを特徴とする方法である。

【0014】また、本発明はアクセスポイントのチェック方法として捉えることができる。このアクセスポイントのチェック方法は、コンピュータ装置を無線によりネットワークへ繋ぐため、ネットワークに接続されるアクセスポイントをチェックする方法であって、ネットワークに対してアクセスが許可されたアクセスポイントの許可リストを取得するステップと、コンピュータ装置により認識されたアクセスポイントの検出リストを取得するステップと、許可リストと検出リストを比較し、検出リストに含まれるアクセスポイントのうち、許可リストに含まれない未登録アクセスポイントを認識するステップと、許可リストに含まれるアクセスポイントの設置箇所を登録するステップと、コンピュータ装置のスキャナによって検出されたアクセスポイントからの信号の強度を取得するステップと、強度に基づき、未登録アクセスポイントの設置箇所を算出するステップと、を有することを特徴とする方法である。

【0015】さらに本発明はコンピュータに実行させるプログラムとして捉えることができる。このプログラムは、ネットワークに接続されたアクセスポイントと無線通信可能なコンピュータ装置に実行させるためのプログラムであって、無線通信可能な帯域の電波をスキャンする手順と、スキャナによって検出されたアクセスポイントのリストを記録する手順と、リストをネットワークを介して送出する手順と、アクセスポイントから発生する振動の強度を取得する手順と、強度をネットワークを介して送出する手順と、を備えたことを特徴とするプログラムである。

【0016】また本発明のプログラムは、コンピュータ装置を無線によりネットワークへ繋ぐため、ネットワークに接続されるアクセスポイントをチェックするプログラムであって、ネットワークに対してアクセスが許可されたアクセスポイントの許可リストを取得する手順と、

コンピュータ装置により認識されたアクセスポイントの検出リストを取得する手順と、許可リストと検出リストを比較し、検出リストに含まれるアクセスポイントのうち、許可リストに含まれない未登録アクセスポイントを認識する手順と、許可リストに含まれるアクセスポイントの設置箇所を登録する手順と、コンピュータ装置のスキャナによって検出されたアクセスポイントからの信号の強度を取得する手順と、強度に基づき、未登録アクセスポイントの設置箇所を算出する手順と、を有することを特徴とするプログラムである。

【0017】その他、本発明は、プログラムを記憶した記憶媒体や、コンピュータ装置に接続可能な無線 LAN 用デバイスを提供することもできる。

【0018】

【発明の実施の形態】以下、添付図面に示す実施の形態に基づいて本発明を詳細に説明する。図1は、本実施の形態における無線通信を利用した LAN (Local Area Network) システム (ネットワークセキュリティシステム) を説明するための構成図である。図1に示す LAN システムでは、ユーザの使用する端末であるクライアント (コンピュータ装置) 10a、10b、10c、10d、10e (以下、10a～eと略する場合がある) と、システム管理者の使用する端末であるコントローラ (コンピュータ装置) 20と、アクセスポイント (以下、APと言) AP#A、AP#B、AP#C、AP#D (以下、AP#A～Dと略する場合がある) が備えられている。クライアント 10a～eは、AP#A～Dを介してネットワークに接続可能とされている。また、コントローラ 20は有線によってネットワークに接続されている。但し、コントローラ 20もAP#A～Dを介してネットワークに接続されるものであってもよい。

【0019】図2は、クライアント 10a～eの構成を示した図である。図2に示すクライアント 10a～eは、CPU等の演算処理部 (認識部) 11と、メモリ 12と、HDD (Hard Disk Drive、記憶部) 13と、ユーザからの入力を受け付け、ユーザに対してデータを出力する入出力部 14と、ネットワークを介して外部とデータの送受信を行う送受信部 (認識部) 15を備えている。さらに送受信部 15は、APをサーチする機能を有するAPサーチ部 16と、取得したAPリストをコントローラ 20へ送出する機能を有するAPリスト送出部 17と、アンテナ 18とを備えている。また、HDD 13は、取得したAPリストを保存するAPリスト記憶部 19を備えている。

【0020】なお、図示していないが、クライアント 10a～eが有する送受信部 15は、アンテナ 18に連絡しているパワー増幅器、RF / IF コンバータ・シンセサイザ、I / Q モジュレータ・デモジュレータ、ベースバンドプロセッサ、電波の送受信をコントロールするメディア・アクセス・コントローラ等を備えている。これ

らはLANカードまたはLANボードとして、例えばIEEE802.11の規格に準拠したものであり、例えば2.4GHz帯の電波を使うもの、5GHz帯の電波を使うもの、赤外線を使うもの等を使用することができる。

【0021】図3は、コントローラ20の構成を示した図である。図3に示すコントローラ20は、CPU等の演算処理部21と、メモリ22と、HDD23と、ユーザからの入力を受け付け、ユーザに対してデータを出力する入出力部24と、ネットワークを介して外部とデータの送受信を行う送受信部25を備えている。さらに、演算処理部21は、取得したAPリストと登録されているAPリストを比較する機能を有するAPリスト比較処理部(抽出部)26を備えている。また、HDD23は、接続を許可されたAPのリストを登録したAPリスト登録部(格納部)27を備えている。そして、送受信部25は、クライアント10a～eから送出されたAPリストを受信する機能を有するAPリスト受信部(収集部)28を備えている。

【0022】なお、上記のクライアント10a～eやコントローラ20は、ユーザが使用するコンピュータ装置であって、例えばノートブック型PC(Personal Computer)や、デスクトップ型PCや、PDA等であり、これらのコンピュータ装置が備えるその他の部材を有することができる。また、クライアント10a～eおよびコントローラ20は互いに同じコンピュータ装置であってもよく、または異なるコンピュータ装置であってもよい。

【0023】通常、無線LANにより外部とのデータ送受信を行う場合、クライアント10a～eの送受信部15はデータの送受信を確実に行うために、定期的にAPの探索を行う。APの探索では、まず所定周波数の電波でスキャンを行い、通信を確立できるAPを見つける。そして、そのAPとのデータ送受信ができることがAPとクライアント10a～eとの間で確認が取れた後、データの送受信を開始する。本実施の形態におけるLANシステムでは、探索されたAPの情報を基に、不正なAPがネットワーク内に存在することを検出することができる。以下、不正なAPを検出する方法を具体的に説明する。

【0024】図4は、クライアント10a～eにおける処理の流れを示す図である。ここで、クライアント10a～eにおける処理は、クライアント10a～eにインストールされたコンピュータ用のプログラムを実行することによって行われる。なお、クライアント10a～eは同じプログラムに基づいて処理を行うので、クライアント10aを例に挙げて説明する。

【0025】まず、HDD13のAPリスト記憶部19に記憶されているAPリスト(以前にAPのサーチが行われている場合、そのとき得られたAPリスト)を消去

する(ステップS101)。続けて、接続するAPを探すために電波をスキャンしてクライアント10aとへ電波を到達させることができるAPをサーチして見つける(ステップS103)。ここで、APのスキャンおよびサーチについて詳細を説明する。

【0026】図5は、送受信部15のAPサーチ部16によるスキャンおよびAPのサーチについての処理の流れを説明する図である。まず、電波のチャンネルナンバー(以下、チャンネルNo.)を1に設定する(ステップS111)。この設定において、クライアント10aは、アンテナ18を介してビーコンを受信できたか否かを判断する(ステップS113)。ビーコンを受信できなかったと判断した場合、後述のステップS117の処理を行う。一方、ビーコンを受信したと判断した場合、通信相手を特定するための識別番号であるSSID(Service Set Identification)とビーコンの信号強度をAPリスト記憶部19のAPリストに追加する(ステップS115)。例えばクライアント10aの場合、図1に示すように、クライアント10aの近辺に位置するAPであるAP#AおよびAP#BがAPリスト記憶部19に記憶される。

【0027】続いて、スキャンする電波のチャンネルNo.を増加させる(ステップS117)。そして、増加させたチャンネルNo.が、送受信部15が受信できる最大チャンネルNo.より大きいか否かを判断する(ステップS119)。チャンネルNo.が最大チャンネルNo.より大きくないと判断した場合、ステップS113へ戻って同様の処理を行う。一方、チャンネルNo.が最大チャンネルNo.大きいと判断した場合、スキャンおよびAPのサーチの処理を終了する。

【0028】以上のようにして得られた、APリストを、図4に示すように、送受信部15のAPリスト送出部17によりコントローラ20へ送出する(ステップS105)。そして、所定の待機時間(t)が経過するのを待機し(ステップS107)、待機が終了すると、再度ステップS101へ戻って処理を開始する。このように、スキャンおよびAPのサーチ処理においては、クライアント10a～eにおいて、それぞれ電波の受信ができるAP、すなわち認識できるAPのチャンネルと、そのAPからの信号強度の情報を受信する。そして、各クライアント10a～eは、図1に示すようにAPリストを取得する。

【0029】図6は、コントローラ20における処理の流れを説明する図である。ここで、コントローラ20における処理は、コントローラ20にインストールされたコンピュータ用のプログラムによって行われる。まず、各クライアント10a～eから送信されたAPリストを送受信部25のAPリスト受信部28にて受信する(ステップS201)。ここで受信したリストは、メモリ22上に一時的に記憶される。そして、待機時間(t)が

経過したか否かを判断する(ステップS203)。この待機時間(t)は、複数のクライアント10a～eから時を同じくせず送信されてくるAPリストを、できるだけ多くのクライアント10a～eから受信するためである。待機時間(t)は、例えば1時間おきに設定することができる。ステップS203において、待機時間(t)が経過していないと判断すると、ステップS203の処理が再度行われる。

【0030】一方、ステップS203において待機時間(t)が経過していると判断すると、受信したAPリストの集合体である収集APリストと、HDD23のAPリスト登録部27に登録されている管理用APリストとの比較をAPリスト比較処理部26により行う(ステップS205)。管理用APリストは、ネットワークへのアクセスを許可された真正なるアクセスポイントのリストであって、管理者APリスト中のアクセスポイントは、ネットワークに接続されているアクセスポイントと一致することが確認されているものである。管理用APリストは、例えばシステム管理者により作成される。その他、真正なるアクセスポイントは、各クライアント10a～e等より認証の要求がなされたアクセスポイントであって、システム管理者により真正なアクセスポイントであると認証されたものであってもよい。

【0031】ここで、図7(a)に各クライアント10a～eから受信したAPリストの一例を示し、(b)に収集APリストとAPリスト登録部27に登録されている管理用APリストのデータの一例を示す。図7(a)に示すように、各クライアント10a～eから収集したAPリストから、実際にネットワークに接続しているAPのデータを、収集APリストとして取得する。そして、収集APリストと登録APリストとを比較して、収集APリストのうち、登録APリストに登録されていないAP、すなわち不正APを抽出する。図7(b)に示す場合は、登録されていないAPとしてAP#Cが抽出される。

【0032】続けて、不正APの検出処理に基づき、不正APがあるか否かを判断する(ステップS207)。不正APは無いと判断した場合、ステップS201へ戻って処理を続ける。不正APがあると判断した場合、コントローラ20のユーザに対して入出力部24を介して警告を発する(ステップS209)。その後、ステップS201に戻って処理を続ける。

【0033】ここで、ステップS209における警告では、不正APの存在と共に、不正APの存在箇所を推定して提示することができる。例えば、コントローラ20のHDD23にネットワークに接続可能である正規に登録されたAPの設置箇所を示した構成図を記録し、クライアント10a～eから受信したAPリストには、それぞれのAPに対する信号強度を含ませる。この場合、正規のAPの設置箇所から、どの程度離れた位置にそのク

ライアント10a～eが存在するかを認識することができ、さらにクライアント10a～eによって認識された不正APについての信号強度を基に、不正APの大よその位置を掴むことが可能となる。このようにしてコントローラ20を介して警告と不正APの位置情報を得ることで、その情報を基に不正APを探し出し、その不正APの撤去を行うことが可能となる。

【0034】以上のように、本実施の形態では、無線LANネットワークに接続しているクライアント10a～eにより、クライアント10a～eが認識できるAPのデータが送出され、そのリストに載ったAPを予め登録されたAPと比較することで、不正なAPを簡単に検出することができる。従来の無線LANネットワークでは、クライアント10a～eは使用できるAPを認識するためサーチを行い、クライアント10a～eに電波が届くAPの認識を行っていたが、データの送受信を行うAPを特定するだけで処理を終了していた。そこで本実施の形態では、クライアント10a～eが得た情報を収集して利用することで、簡単に且つ確実に不正APの検出を可能とした。

【0035】また、本実施の形態では、APリストを取得する処理は、クライアント10a～eとして通常に使用するコンピュータ装置に所定のプログラムをインストールするだけで、実行することができる。また、コントローラ20に対しても同様に所定のプログラムをインストールして正規なAPを登録するだけで、不正APの検出を行うことができる。よって、本実施の形態では、低コストで簡単に不正APの検出を行うことが可能である。

【0036】なお、上記実施の形態において、コントローラ20の代わりに、クライアント10a～eのいずれかにコントローラ20の機能を備えさせることが可能である。その場合、コントローラ20に導入するプログラムを、クライアント10a～eのいずれかにインストールすればよい。さらに、各クライアント10a～eのHDD13に登録された正規のAPリストを記憶させ、各クライアント10a～eにおいて不正APを検出するものであってもよい。

【0037】また、上記実施の形態においては、各クライアント10a～eからコントローラ20へ対して自動的にAPリストが送出されているが、本実施の形態はこれに限定されない。例えば、コントローラ20側から各クライアント10a～eにアクセスして要求することで、APリストを取得するものであってもよい。この場合、クライアント10a～eが検出するAPリストの取得は定期的に行うこともできるが、システム管理者が取得を希望する時、例えば1日に2～3回任意に取得することも可能である。

【0038】さらに、上記実施の形態においては、クライアント10a～eがAPリストを取得する処理のタイ

ミングを決める間隔を待機時間（t）とし、コントローラ20がクライアント10a～eから受信したAPリストを比較処理するタイミングを決める間隔と同じく待機時間（t）としているが、本実施の形態はこれに限定されない。例えば、クライアント10a～eが頻繁に移動して使用されることを考慮した場合、クライアント10a～eはより接続しやすいAPを頻繁に探す、即ち頻繁にAPリストを入手する。それに対してこのAPリストはコントローラ20に対して頻繁には送出せず、例えば数時間おきに送出するものであってもよい。また、頻繁に送出するものであっても、コントローラ20における待機時間（t）を長く設定することで、不正APの検出の回数を制御することもできる。

【0039】また、上記実施の形態においては、検出された不正APは位置を検出されて撤去されているが、本実施の形態はこれに限定されない。例えば、その不正APが接続しているルータを操作することで、不正APとのデータの送受信を禁止させるものであってもよい。また、不正APが存在することのみ警告を発し、不正APの位置の検出はコントローラ20以外で行われるものであってもよい。

【0040】その他、上記実施の形態においては、導入されたプログラムによってクライアント10a～eとコントローラ20における処理を実行しているが、本実施の形態はこれに限定されない。例えば、プログラムを導入する代わりに、クライアント10a～eに接続される無線通信用デバイス（無線LAN用PCカードやボード等）に、取得したAPリストを定期的にコントローラ20に対して送信する機能を持たせることもできる。この場合、無線通信用デバイスをクライアント10a～eに接続するだけで、不正APを検出するためのクライアント10a～eとしての機能を果たすことが可能となる。また、コントローラ20についても同様に、ネットワークに接続するためのデバイスにコントローラ20としての機能を持たせることができる。

【0041】なお、本実施の形態で示したような処理を行うためのプログラムは、以下のような記憶媒体、プログラム伝送装置の形態とすることもできる。すなわち、記憶媒体としては、コンピュータ装置に実行させるプログラムを、CD-ROM、DVD、メモリ、ハードディスク等の記憶媒体に、コンピュータ装置が読み取り可能

となるように記憶させれば良い。また、プログラム伝送装置としては、上記したようなプログラムを記憶させたCD-ROM、DVD、メモリ、ハードディスク等の記憶手段と、この記憶手段から当該プログラムを読み出し、当該プログラムを実行する装置側に、コネクタ、あるいはインターネットやLAN等のネットワークを介して当該プログラムを伝送する伝送手段とを備える構成とすれば良い。これ以外にも、本発明の主旨を逸脱しない限り、上記実施の形態で挙げた構成を取捨選択したり、他の構成に適宜変更することが可能である。

【0042】

【発明の効果】このように本発明によれば、無線ネットワークエリア内に設けられた不正なアクセスポイント（AP）を簡単に検出することができる。

【図面の簡単な説明】

【図1】 本実施の形態におけるLANシステムを説明するための構成図である。

【図2】 クライアントの構成を示した図である。

【図3】 コントローラの構成を示した図である。

【図4】 クライアントにおける処理の流れを示す図である。

【図5】 クライアントのAPサーチ部によるスキャンおよびAPのサーチについての処理の流れを説明する図である。

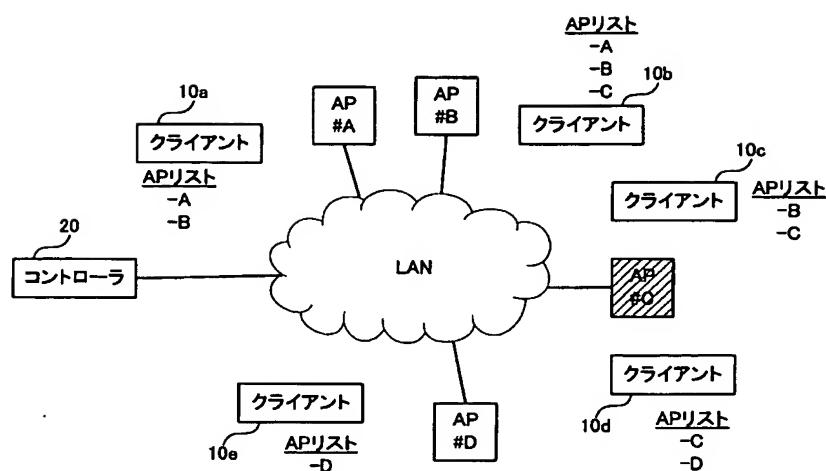
【図6】 コントローラにおける処理の流れを説明する図である。

【図7】 (a)は各クライアント10a～eから受信したAPリストの一例を示す図であり、(b)は収集APリストとAPリスト登録部に登録されている管理用APリストのデータの一例を示す図である。

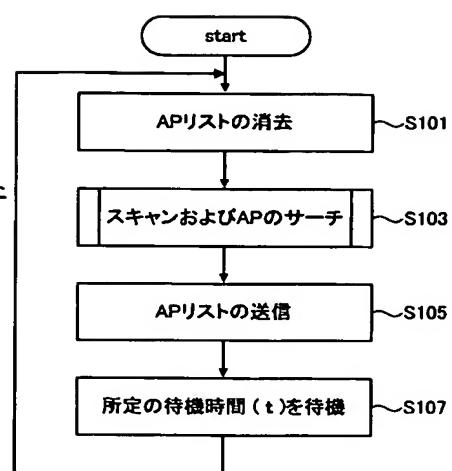
【符号の説明】

10a、10b、10c、10d、10e…クライアント（コンピュータ装置）、11…演算処理部（認識部）、13…HDD（記憶部）、15…送受信部（認識部）、16…APサーチ部、17…APリスト送出部、18…アンテナ、19…APリスト記憶部、20…コントローラ（コンピュータ装置）、21…演算処理部、23…HDD、25…送受信部、26…APリスト比較処理部（抽出部）、27…APリスト登録部（格納部）、28…APリスト受信部（収集部）、AP#A、AP#B、AP#C、AP#D…アクセスポイント

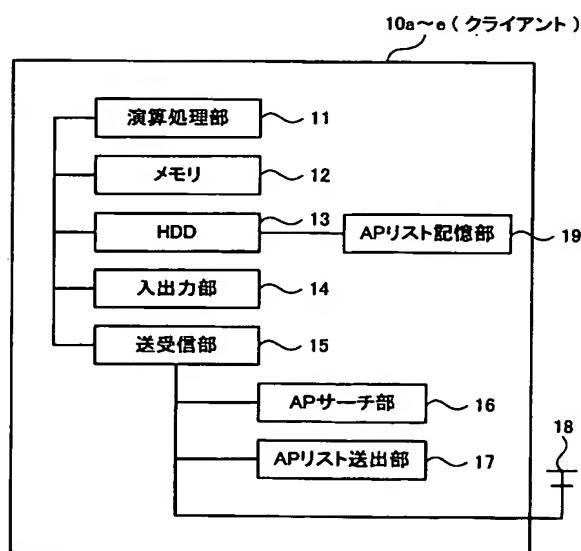
【図1】



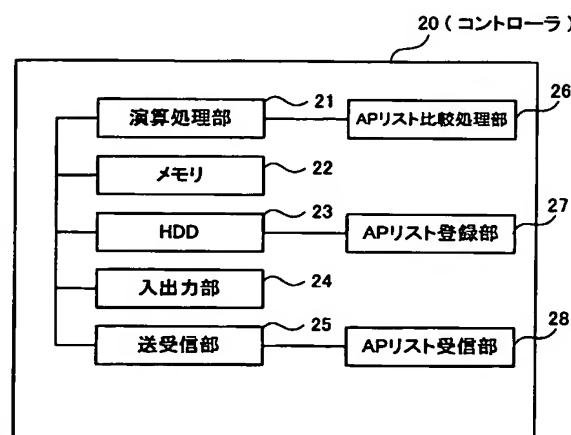
【図4】



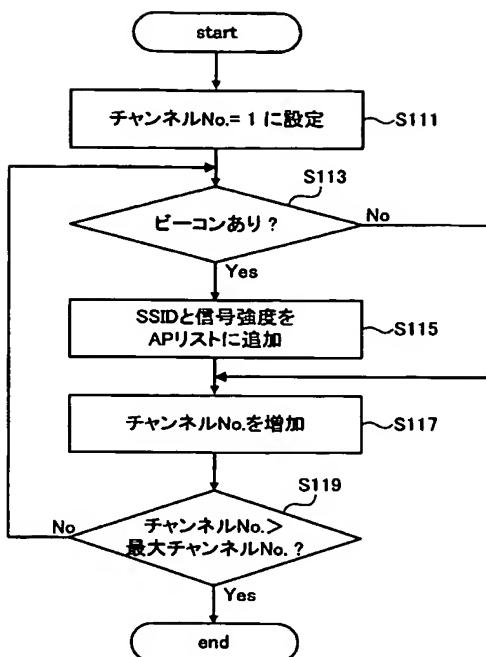
【図2】



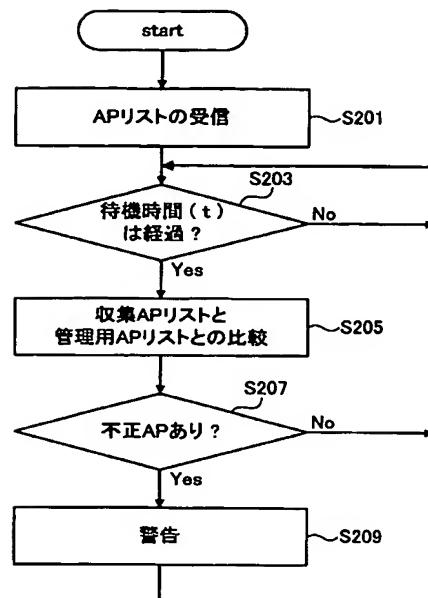
【図3】



【図5】



【図6】



【図7】

(a)

クライアント名	APリスト
クライアント10a	A, B
クライアント10b	A, B, C
クライアント10c	B, C
クライアント10d	C, D
クライアント10e	D

→ 集収APリスト
A, B, C, D

(b)

集収APリスト	A, B, C, D
登録APリスト	A, B, D

フロントページの続き

(72)発明者 藤井 一男
神奈川県大和市下鶴間1623番地14 日本ア
イ・ビー・エム株式会社 大和事業所内
(72)発明者 松永 幸三
神奈川県大和市下鶴間1623番地14 日本ア
イ・ビー・エム株式会社 大和事業所内

(72)発明者 伊藤 雅晴
神奈川県大和市下鶴間1623番地14 日本ア
イ・ビー・エム株式会社 大和事業所内
F ターム(参考) 5K033 AA08 CB01 DA01 DA17 DB20
5K067 AA30 BB21 DD19 EE02 EE10
EE16 FF03 HH23 KK15